Strategy Research Project

Who is Responsible for Defending United States Interests in Cyberspace?

by

Lieutenant Colonel Thomas A. Boone
United States Army

United States Army War College
Class of 2013

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
xx-03-2013	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
Who is Responsible for Defending United States Interests in Cyberspace?

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Lieutenant Colonel Thomas A. Boone
United States Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Professor Brian Gouker
Department of Military Strategy, Planning, and Operations

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.

13. SUPPLEMENTARY NOTES
Word Count: 6,493

14. ABSTRACT

As a nation, the United States of America created the Internet, embraced it, and opened up the potential to link people around the globe, crossing international and cultural boundaries. Americans leveraged the new capability to such a great extent that it has been woven into the fabric of our society, which also provides an avenue for our adversaries to exploit. With such grave concern over potential attacks within the complex cyber environment, which department is responsible to protect United States interests? Presidential Directives have designated the Department of Homeland Security as a government lead while the Department of Defense also has a key role in cyber. In reviewing authorities of each organization and within the context of other contributors to the protection of U.S. interests there is minimal overlap between the two organizations. Current laws limit the potential defense while also not clearly designating roles and responsibilities, while the threat continues to increase.

15. SUBJECT TERMS
Cyber, Legal Authorities

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(Include area code)*
UU	UU	UU	UU	38	

USAWC STRATEGY RESEARCH PROJECT

Who is Responsible for Defending United States Interests in Cyberspace?

by

Lieutenant Colonel Thomas A. Boone
United States Army

Professor Brian Gouker
Department of Military Strategy, Planning, and Operations
Project Adviser

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Abstract

Title:	Who is Responsible for Defending United States Interests in Cyberspace?
Report Date:	March 2013
Page Count:	38
Word Count:	6,493
Key Terms:	Cyber, Legal Authorities
Classification:	Unclassified

As a nation, the United States of America created the Internet, embraced it, and opened up the potential to link people around the globe, crossing international and cultural boundaries. Americans leveraged the new capability to such a great extent that it has been woven into the fabric of our society, which also provides an avenue for our adversaries to exploit. With such grave concern over potential attacks within the complex cyber environment, which department is responsible to protect United States interests? Presidential Directives have designated the Department of Homeland Security as a government lead while the Department of Defense also has a key role in cyber. In reviewing authorities of each organization and within the context of other contributors to the protection of U.S. interests there is minimal overlap between the two organizations. Current laws limit the potential defense while also not clearly designating roles and responsibilities, while the threat continues to increase.

Who is Responsible for Defending United States Interests in Cyberspace?

> A Cyber attack perpetrated by nation states or violent extremist groups could be as destructive as the terrorist attack of 9//11. Such a destructive cyber terrorist attack could paralyze the nation.
>
> —Secretary Leon Panetta

As a nation, the United States of America created the Internet, embraced it, and opened up the potential to link people around the globe, crossing international and cultural boundaries. Americans leveraged the new capability to such a great extent that it has been woven into the fabric of our society, which also provides an avenue for our adversaries to exploit. With such grave concern and potential damage from a cyber attack where has the United States placed the authority and responsibility to protect our national interests? The Department of Homeland Security (DHS) describes their role in the "2010 Bottom-up Review" which details that their authority evolves from the 2002 Homeland Security Act as well as Presidential Directive 23:

> …the Secretary shall lead the national effort to protect, defend, and reduce vulnerabilities of Federal systems (excluding civilian national security systems), and shall provide consolidated intrusion detection, incident analysis, and cyber response capabilities to protect Federal agencies' external access points.[1]

However, the specific legal authorities, which would enable DHS to execute the cyber mission, are still unclear based on their own internal analysis.[2] There are numerous definitions of what is a National Security System depending on the source so the following definition is provided.

> 400 USC § 11103 defines National Security Systems as telecommunications or information system operated by the federal government with the following function, operation or use which involves intelligence, cryptologic activities related to national security, involves command and control of military forces, equipment integral as a part of a

> weapon system, or is critical to the direct fulfillment of military or intelligence missions.[3]

As with new systems and technology, common understanding and definitions are not always apparent. The White House National Security Council provides the following definition of cyberspace from their "Cyberspace Policy Review."

> Cyberspace is defined as the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.[4]

On June 23, 2009, then Secretary of Defense Robert Gates directed U.S. Cyber Command be established to defend the department's networks as well as provide freedom of action in cyberspace.[5] The challenge in the man-made domain of cyber is that of identifying the threat, delineating intent, and then taking action across a generally unregulated space that crosses sovereign national boundaries. Unfortunately the military and government as a whole do not own the vast majority of the networks they currently use today. These open-ended and immature policies concerning banking, private sector communications and infrastructure were mentioned by the Commander of Strategic Command in his congressional testimony of the requirement to "clarify the global roles, responsibilities, expectations, and authorities that contribute to a stable and effective deterrence and assurance" in the cyber domain.[6]

Environmental Challenges

With over 116,000 reported cyber incidents to DHS last year alone, the trend continues to increase in both volume and complexity.[7] Those are only the incidents actually reported to DHS. The ability and low entry cost into the cyber domain increases the number of players from nation-state actors, criminals, terrorists, and random hackers attempting to make a public statement or exploit vulnerabilities. With

the challenge of attribution in cyberspace, how does the U.S. government classify cyber activities as either threats to national security or law enforcement issues? Cyber intertwines real and virtual personas, embedding personal identifiable information into electronic communications that make protection of cyber unique when compared to other domains such as the sea. Cyber has been in existence for roughly three decades as opposed to the Law of the Sea that took over 300 years to develop and reach consensus by the international community.

Complexity and Definition of the Threat

Knowing what originated the malicious activity on a specific network, as well as when the incident actually began on a specific target, can be challenging at best depending on the intent of the attacker. Cyber disruptions in our modern world have become even more critical as our nation's dependence on the network and maintaining connectivity continues to increase. Furthermore, social/political movements or groups such as "Anonymous" include many groups of individuals from "teenagers to anarchists" as "anyone can engage in a malicious act and claim it "Anonymous."[8] Attribution is a key component as the U.S. must be able to quickly see the threat to allow a "calibrated and calculated response", a significant challenge in this environment.[9] Cyberspace has no physical boundaries and is constantly changing, which challenges any efforts to defend this domain.[10] Cyber activity may employ similar techniques to either exploit or attack a network to achieve an effect or purpose. With many common traits in cyber events, it can be challenging to determine if the response should originate from law enforcement or defense officials. Theft, exploitation, publicity, espionage, and damage are only a few of the possible motives for a malicious cyber activity. So with a complex environment, how might we delineate the spectrum of cyber disruptions, which

challenge our national interests? Colonel Gary Brown and Lieutenant Colonel Owen Tullos, USCYBERCOM's Staff Judge Advocate (SJA) and Deputy SJA, provide a potential framework for classification of cyber activities into the three categories of: access operations, cyber attack, and cyber disruption.[11] Access operations would be gaining access via software installation, defeating security measures, and exploiting vulnerabilities while not impacting normal function of the system or the user.[12] On the opposite end of the spectrum from access operations would be cyber attacks, which are "actions in cyberspace whose foreseeable results include damage or destruction of property, or death or injury to persons."[13] In between these extreme actions would fall cyber disruptions, which would be the vast majority of incidents currently experienced within cyber. "Cyber disruption includes actions that interrupt the flow of information or function of information systems without causing physical damage or injury."[14]

The Nature of the Targets

The DHS Strategy for the physical defense of critical infrastructure defines 13 key sectors and five additional key assets, which run the spectrum from agriculture to shipping to nuclear power plants.[15] All of these sectors are dependent on cyber, and therefore also potentially vulnerable to network disruption and attack. These sectors are susceptible to physical attack as well as cyber attack. If destroyed or even degraded these results would negatively impact the U.S. economy. Due to the exponential increases in productivity, people and companies continue to use the Internet without sufficient regard for the potential risks embedded with new technology. Acknowledging that the threat is worldwide, government officials from the UK have admitted that their country's critical infrastructure may have already been completely mapped utilizing cyber intrusions.[16] Of course why would a person go to the trouble to

pull down the extensive designs supporting key infrastructure such as power and water? Two possible options are 1) to save money and time in developing another countries internal infrastructure or 2) to enable an adversary the opportunity to examine and prepare for a disruption or attack. This example demonstrates the complexity in both defending key networks, but also the varied targets potentially available for exploitation.

Civil Rights and Individual Freedom

"The Cyber Sea is the ultimate expression of freedom, as it cannot be constrained by national or international lines drawn on any map or chart."[17] The growth of the interconnectedness of society continues to expand at a break neck pace, reaching all the corners of the world. When looking at the expansion of freedom, one must be concerned about individual rights. Many people have built a virtual persona on the web linked to very tangible aspects of our life such as finances with online banking and the new cashless societies. Several U.S. Congressmen have argued that the Defense Department must be prepared to defend the homeland against attacks in all domains so DoD should have the cyber lead, not DHS.[18] People on the opposing side cite freedom as the primary issue, which is contrary to military intervention and proponency. Recent legislative actions and proposals have created significant privacy concerns and proposed potential minimum standards in cyber security for private business. The U.S. Chamber of Commerce worked openly to challenge legislation that potentially would have directed minimum standards for operators of key infrastructure. The Chamber's position argued that Senate Bill 3414 would "impede U.S. cybersecurity by shifting business resources away from implementing robust and effective security measures and toward meeting government mandates."[19] Legislation should focus on information sharing and liability of companies to enable private public collaboration to

protect critical infrastructure as the U.S. Chamber of Commerce actively identifies the potential of cyber.[20]

Stakeholders in Cyber

As cyber touches all the physical environments of air, space, land, and sea it also crosses political, cultural, and national boundaries. Just from the U.S. perspective, and leaving the international community separate, there are competing interests and ideas as to how best secure cyber. All levels of government from the U.S. Federal government to the local communities all rely on cyber to provide for their citizens. Private and public partnerships pervade as everyone is potentially enabled or disrupted in cyberspace. Retail, manufacturing, and shipping industries depend on reliable and secure access to cyberspace supported by infrastructure enabled through the access to the virtual highways. General Keith B. Alexander, Commander of U.S. Cyber Command (USCYBERCOM) and Director, National Security Agency/Chief, Central Security Service (NSA/CSS) described the U.S.'s overall preparation for a cyber threat as a "3 out of 10."[21] He went on to address specific issues such as the speed of detection and associated response, shortfalls in standards.[22] The key issue he identified was the unresolved issue of private/public information sharing about the threats.[23]

Current Responsibilities and Authorities

Options must be explored as current laws enable or limit operations within cyber and the protection of U.S. interests. Some have likened cyber to control of U.S. airspace by the Federal Aviation Administration (FAA), which controls the air. While North American Aerospace Defense Command (NORAD) stands ready to provide military assistance at the request of the FAA. Their purpose as a bi-national organization is "charged with the missions of aerospace warning and aerospace control

for North America."[24] While U.S. Cyber Command has been charged to "operate and defend the Department of Defense information networks and when directed, conducts full-spectrum military cyberspace operations (in accordance with all applicable laws and regulations) in order to ensure U.S. and allied freedom of action in cyberspace, while denying the same to our adversaries."[25] Key differences are stark when looking at the two organizations. USCYBERCOM's mission includes the context of laws and regulations and also is more limited since the defense mission only applies to military networks. NORAD's mission is more direct and clear in "control" so perhaps this comparison is inadequate in reviewing the use of military to defend the homeland in cyberspace.

A better model would be to look at jurisdiction of bank robbery. The Federal Bureau of Investigation (FBI) has maintained the lead of such events since 1930, but also works with local authorities on cases.[26] At the time of the physical robbery, bank security personnel react to the incident, as they are first on the scene as robbers enter a bank. Alerts go out and local police respond to the incident with special units such as quick reaction teams or Special Weapons and Tactics (SWAT) units. Despite the FBI having investigative lead and offices throughout the U.S., they cannot respond rapidly to every incident. The FBI will investigate and coordinate with local authorities to solve the crime. In this example all participants are part of the greater law enforcement community, but all react to the bank robbery in there own ways: private security taking the initial lead in protecting the bank while local police patrol the local community and ultimately the FBI is watching for larger trends and threats to banks. Rules and laws will determine the lead for the investigation in the long run, but this does not stop the initial

reaction by each organization to protect the bank at the moment of crisis. In the extreme case of cyber attacks, precedence has not been established to provide the specific legal authorities to enable a consolidated and coordinated response. General Keith B. Alexander, Commander USCYBERCOM and Director NSA/CSS recently stated that "I'm concerned that attacks (such as initiated against Saudi Arabia's state owned oil company, Aramco) like that are coming, and we're spending a lot of time talking about what we should do, when we should just do it."[27]

Authorities Defined

Legal authorities allow a government agency to do its mission and take action. As a construct, authorities can be categorized as primary authorities and secondary authorities. Those authorities based in law and are binding such as our Constitution, federal legislation, presidential directives, and case law serve as the basis for the primary authority. A federal agency would also derive secondary authorities from documents that interpret, clarify, or provide implications from the original primary documentation. Examples of secondary authorities would be an agency's plan, legal texts, and plans derived from the primary binding document, which may have not provided the required specificity.[28]

Department of Homeland Security Authorities

Executive Order 13231 (OCT 2001): Critical Infrastructure Protection in the Information Age

President George W. Bush's order assigned cyber oversight responsibility, policy development, principles, and guidelines to the OMB across the entire executive branch, but expressly excludes national defense systems.[29] Furthermore, this executive order established the National Infrastructure Advisory Council (NIAC) as central component

which “shall provide the President advice on the security of information systems for critical infrastructure supporting other sectors of the economy: banking and finance, transportation, energy, manufacturing, and emergency government services.”[30] Ultimately the NIAC, based on authority from the President, provides guidance and direction to DHS from the operators of critical infrastructure. [31] The NIAC is currently composed of key strategic leaders from corporations such as FedEx, Northrop Grumman, Dow Chemical, Clorox Company, Southwest Airlines, and government leadership such as the Police Commissioner City of New York.[32] Ultimately this provision enables bottom-up input to DHS as well as open communication with those operators who have the most intricate knowledge of their specific element of key infrastructure.

Homeland Security Act (HSA)(November 2002)

The Homeland Security Act created DHS from an amalgamation of 23 separate federal agencies and also provided applicable authorities. 6 USC §112 empowers DHS to work with federal laboratories to identify the “best available technologies for homeland security mission” and also “promote” and “develop public-private partnerships.”[33] DHS also is tasked to “develop a comprehensive national plan for securing the key resources and critical infrastructure” to include the elements of cyber as it impacts banking, communications, and power production.[34] Another key authority provided to DHS supports information sharing of both law enforcement and intelligence information across all levels of government and the private sector with concern to homeland security.[35] Specific to cybersecurity, this key public law enables DHS to share “analysis and warnings related to threats to, and vulnerabilities of, critical information systems” and for DHS to develop a “national technology guard’ which links

the Department to private sector.[36] This ability to share provides the conduit for the Defense Department to pass along key information concerning cyber to the private sector, but does not provide legal protection for companies to share information with the government.

Federal Information Security Management Act (FISMA) (December 2002)

FISMA directed that the Office of Management and Budget (OMB) provide guidance and policy to direct all "e-government" initiatives, as well as address risk to federal agency information and systems.[37] National security systems such as military command and control, intelligence, crytopgraphic, and weapon systems were expressly not included within FISMA's authorities to OMB.[38] OMB later issued guidance on the implementation of FISMA which "authorized DHS to provide operational support to federal agencies in securing their systems and networks and monitor agency progress to ensure compliance with FISMA requirements."[39] FISMA clearly delineated the responsibilities by excluding National Security Systems from the responsibility of DHS.

Executive Order 13286 (February 2003) Amendment of Executive Orders, and Other Actions, in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security

President George W. Bush ordered adjustments to already active executive orders. EO 13286 amends previous EO 12382 moving the responsibility of the President's National Security Telecommunications Advisory Committee (NSTAC) to DHS.[40] NSTAC is a collaborative body "of up to 30 industry chief executives from major telecommunications companies, network service providers, information technology, finance, and aerospace companies."[41] This executive order also transferred the functions of The National Security and Emergency Preparedness Telecommunications Functions as per EO 12472 to the newly formed DHS. The primary function of the

National Communications System (NCS) is to ensure the national telecommunications infrastructure is "satisfying priority telecommunications requirements under all circumstances through use of commercial, government and privately owned telecommunications resources."[42] Key attributes identified are "hardness, redundancy, mobility, connectivity, interoperability, restorability and security" to allow "the survivability of national security and emergency preparedness telecommunications in all circumstances, including conditions of crisis or emergency."[43] A natural extension of the executive order's requirement for redundant and reliable government communication went to support DHS's responsibility in cyber. This Presidential directive brought more of the responsibilities and capabilities under the DHS purview by setting the Department as the lead for cyber.

HSPD-7 (December 2003) Critical Infrastructure Identification, Prioritization, and Protection

In the broadest application, the President directed a policy to define "key and critical resources" with the intent to protect them from attacks by terrorist incidents. HSPD-7 identifies DHS as "responsible for coordinating the overall national effort to enhance the protection of the critical infrastructures and key resources of the United States".[44] With respect to cyber, HSPD-7 specifies "The (DHS) Secretary will continue to maintain an organization to serve as a focal point for the security of cyberspace."[45] With this responsibility, as the lead agency, DHS must share threat information, assist with vulnerability assessments, support defensive measures, and develop contingency operations. DHS is directed to coordinate with other federal agencies per sector specific assignments such as DoD to lead the effort on defense industrial base. "The Secretary will continue to maintain an organization to serve as a focal point for the

security of cyberspace."[46] The Presidential Directive assigned sectors to specific departments based on the unique requirements for each with a focus to "collaborate", "conduct or facilitate vulnerability assessments", and "encourage risk assessments of the sector."[47] Responsibilities for each of the departments are below:

1. Department of Agriculture – agriculture, food (meat, poultry, egg products)

2. Department of Human Services – public health, healthcare, and food (other than meat, poultry, egg products)

3. Environmental Protection Agency – drinking water and water treatment systems

4. Department of Energy – energy, including the production refining, storage, and distribution of oil and gas, and electric power except nuclear power facilities

5. Department of Treasury – banking and finance

6. Department of Interior – national monuments and icons

7. Department of Defense – defense industrial base

These sectors represent the structure of U.S. interests in cyber, which impacts the countries overall strength. Attacking or disrupting these interests represents a significant threat to the U.S. in both physical loss and degradation of the nation's reputation and intellectual property. While assigning sectors to specific departments, the Presidential Directive maintains a network approach to solving the problem, as it does not assign an empowered executive agent with real authority to synchronize the defense. The directive uses terms such as "Focal Point" to provide the closest definition that DHS has the lead.

NSPD-54 / HSPD-23 (January 2008) Cyber Security and Monitoring

NSPD-54 / HSPD-23 takes NSPD-7 a step further in providing greater clarity on the role of DHS. A key shortfall is the exclusion of defending the federal government's information systems, as this directive was outwardly focused on the nation's critical infrastructure.[48] The key components of this directive were the authorization of DHS as the lead to establish standards for the agencies of the executive branch while coordinating with the Office of Management and Budget (OMB).[49] Furthermore, under already established authorities such as HSPD-7, DHS serves as the lead for critical infrastructure to prevent degradation and damage across cyberspace. This authority was expanded in NSPD-54/HSPD-23 as it codified the already published Comprehensive National Cybersecurity Initiative (CNCI). A key addition with this directive was the guidance for DHS to advance private and public efforts in the defense of the nation's key and critical infrastructure within the realm of cyber.[50] While the guidance allows DHS to work public/private partnerships it does not have the authority to legally protect private organizations and companies from lawsuits if they choose to share data on cyber disruptions and threats with the federal government. Legislation is needed to provide the construct and protection to private organizations that in early 2013 has still not been resolved by Congress.[51] This lack of legal protection undercuts this Presidential initiative and guidance provided to DHS.

Presidential Executive Order (February 2013) Improving Critical Infrastructure Cybersecurity

President Barack Obama updated the U.S. Policy to ensure that the country improves the "security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency."[52] Key directives on policy

development of information sharing both unclassified and classified cyber reports were included with the Attorney General, DHS, and Director of National Intelligence coordinating this effort.[53] The President goes on to encourage additional voluntary participation by critical infrastructure in the Enhanced Cybersecurity Services Program.[54] Without additional congressional action, there can be no requirement for owners of critical infrastructure to participate in the program.

Federal Bureau of Investigation (FBI)

The USA Patriot Act (Public Law 107-56, USC § 506(a)) amended the 1984 Counterfeit Access Device and Computer Fraud and Abuse Act giving primary investigative authority to the FBI for cyber criminal activity. One exception was offenses impacting the United States Secret Service which remains with the Attorney General. The U.S. Secret Service was given primary investigative authority over fraud cases to include those involving computers.[55] The 1984 Act classified unauthorized access to computers as a federal crime. This included certain categories such as national security information, banking and credit, and information accessed from a "protected computer". "A protected computer is one used by or for a financial institution, the federal government, or one used in interstate or foreign commerce and communication."[56] These laws classify most of the potential cyberspace actions from introduction of malware, exploitation, theft, and destruction as a federal crime.

National Institute of Standards and Technology (NIST)

NIST is a non-regulatory directorate under the Secretary of Commerce who provides standards, technology, and scientific research with the goal of increasing the U.S. economic security and increasing our national quality of life.[57] Authorities enabling NIST to create standards and guidelines come from several key legal documents.

FISMA allows research in protection of information and also determining vulnerabilities in systems. The 2002 Cyber Security Research and Development Act tasked NIST to develop checklists to minimize the potential threat to systems both hardware and software used across the federal government.[58] Homeland Security Presidential Directive 7 empowers NIST with authorities derived from Commerce Department to "improve technology for cyber systems and promote other critical infrastructure efforts" as they work with private, academic, and government organizations.[59] President Obama's latest executive order directs the Secretary of Commerce to further direct NIST to develop a "Cybersecurity Framework" with the goal of reducing the overall cyber threat to critical infrastructure.[60]

Executive Branch Cybersecurity Coordinator

President Barack Obama ordered the creation of a new position, Special Assistant to the President and Cybersecurity Coordinator to lead the interagency development of policy and strategy.[61] President Obama initially appointed Howard A. Schmidt to serve as the White House coordinator as of December 2009, now Michael Daniel serves in the same capacity. This coordinator has driven the cyber threat to the forefront of the news to highlight the importance of protecting individual computers. Congressional leaders have questioned the appointment of a "Cyber Czar" within the White House as the individual will have no authority to act independently and is beyond congressional appointment.[62]

Department of Defense (DoD)

Despite specific legislation concerning DoD operations in cyberspace, the Department has applied applicable laws, directives, and orders in the application of defensive operations within the cyber domain. General Keith B. Alexander in his

prepared statement before the Senate Armed Services Committee, articulated that DoD as a whole is one of the three key cyber members (in addition to DHS and the FBI).[63] General Alexander went on to specify DoD responsibilities: “detection, prevention, and defense in foreign space, foreign cyber threat intelligence and attribution, security of national security and military systems; and, in extremis, defense of the homeland if the Nation comes under cyber attack.”[64]

U.S. Code Title 10

Title 10 provides the foundational authority empowering the Secretary of Defense, as well as subordinate commanders across the military, to take action on behalf of the President as Commander in Chief. In short, Title 10 covers the roles and responsibilities across DoD.[65] Title 10 empowers the Secretary with the “authority, direction, and control over the Department of Defense” and “performs any of his functions or duties, or exercises any of his powers through, or with the aid of, such persons in, or organizations of, the Department of Defense as he may designate.”[66] Title 10 Authority flows from the Secretary of Defense and through the Unified Command Plan (UCP), which includes the sub-unified command of U.S. Cyber Command providing clear and unambiguous authority to the Commander.

Title 10 provides limitations and guidance to the DoD in military support to law enforcement agencies such as information sharing. Key provisions allow DoD to support law enforcement officials with specific intelligence relevant to drug enforcement as a specific example.[67] Perhaps most importantly Title 10 directs DoD to consider the requirements of civilian law enforcement when planning as well as executing military training and operations, which may offer some options for cyber enforcement.[68] Extending this military authority to act within the cyber domain is consistent with current

Title 10 authorities. There are other specific circumstances identified within Title 10 where DoD has greater authority in handling an event involving Weapons of Mass Destruction (WMD) if the Attorney General requests support. Congress could choose to legislate changes within Title 10 to broaden DoD's support in cyber just as they have in both drug enforcement and handling WMD incidents.

U.S. Code Title 50

Title 50 provides the Secretary of Defense with all authority over the Intelligence Community within the Department of Defense to include the National Security Agency (NSA) and other "Combat Support Agencies". Specified requirements include the responsibility to provide intelligence to fulfill the "requirements of unified and specified combatant commanders and of joint operations."[69] This authority enables NSA to execute signals collection and analysis in support of U.S. Cyber Command as a sub-unified command with all appropriate foreign intelligence linking the intelligence collection to the military operations working with Title 10 authorities. "Title 10 and Title 50 are mutually reinforcing authorities" as Title 50 clarifies the Secretary of Defense's authority in Title 10 over the entire DoD intelligence apparatus.[70] This complimentary role in authorities fully supports the current duel nature of command as executed by General Keith B. Alexander as the Commander of USCYBERCOM and Director of NSA/CSS.

Posse Comitatus Act of 1879

This long-standing Act prohibits the use of the military in carrying out civilian law enforcement within the United States as a result of the significant actions taken by the Army in the south at the conclusion of the U.S. Civil War.[71] These limitations do not include the routine actions carried out on a federal reservation or installation. Congress

provided three separate statutory exceptions by giving the Coast Guard law enforcement authority, providing the President the authority to call out the military in response to an insurrection or domestic violence, and finally it does allow sharing of information and also equipment to civilian law enforcement agencies. [72] Additional legislation in 1981 provided detailed authority and restrictions in the authority of the military to support law enforcement at all levels in the type of information and equipment.

Executive Order 12333 (December 1981) United States Intelligence Activities

This executive order issued by President Ronald Reagan serves as the primary basis for intelligence operations and restrictions for the last 32 years. The overarching goal was for the Intelligence Community to provide intelligence in support of decision-making in the "conduct and development of foreign, defense, and economic policy, and the protection of the United States national interests from foreign security threats."[73] DoD was designated as the executive agent for the entire U.S. federal government with regard to signals intelligence and information assurance. NSA's responsibilities were articulated as the "unified organization for signals intelligence" and further delegated to execute the responsibilities of the Secretary of Defense "as the executive agent for the communications security of the United States Government."[74]

National Security Directive-42 (July 1990) National Policy for the Security of National Security Telecommunications and Information Systems

With this directive, the President established the Committee on National Security Systems (CNSS) to consider, develop, staff, and implement policy with concern to the entire national security systems architecture, although systems controlled by the Director of Central Intelligence (DCI) are exempted.[75] CNSS was previously known as

the National Security Telecommunications and Information Systems Security Committee (NSTICCS) which was created in 1953.[76] The Secretary of Defense serves as the Executive Agent for the committee while the Director of NSA is the National Manager with responsibility to report to the Executive Agent.[77] The Assistant Secretary of Defense Networks and Information Integration/Chief Information Officer (ASD/NII/CIO) chairs the CNSS with representatives across 21 federal departments / agencies as voting members. As the National Manager, General Keith B. Alexander exercises oversight of CNSS from his position as Director of NSA while combined with his Title 10 authorities as Commander of USCYBERCOM.

Executive Order 13231 (October 2001): Critical Infrastructure Protection in the Information Age

President George W. Bush assigned responsibility for the National Security Information Systems to the Secretary of Defense and the Director of Central Intelligence (DCI) in Executive Order 13231. Specifically this order articulated that "the Secretary of Defense and the DCI shall develop policies, principles, standards, and guidelines for the security of national security information systems."[78] So with this presidential order, the Secretary of Defense has been given explicit authority and responsibility for the department's information systems.

Assessment

Considering the dramatic pace of change in cyber and understanding the current authorities of the major contributors to the U.S. cyber effort, is this adequate to address President Obama's "International Strategy to Secure Cyberspace" published May 2011?[79] DHS has the generic responsibility and authority as "the lead federal agency", but the current legislation does not fully empower the Secretary of Homeland Security to

act. DoD remains limited to the protection of their internal networks but even the unclassified networks, which carry for example payroll information, may not meet the definition as National Security Systems. Federal Law, specifically the Telecommunications Act of 1984, hinders further advancement of action, since most disruption and attack on U.S. networks are considered law enforcement actions and therefore within the FBI's jurisdiction. A review of current law identifies minimal overlap between DHS and DoD as the structure utilized in defense of key and critical infrastructure limits DoD direct involvement to the defense industries. In fact the February 2013 Presidential Executive Order on Improving Critical Infrastructure Cybersecurity and PPD 21 provide no significant changes to DoD responsibilities, while it provides requirements for other executive agencies such as DHS and Secretary of Commerce.[80] The September 2010, DoD / DHS memorandum of agreement provided the common agreement on exchanging personnel between the departments and built a structure to increase collaboration within the current legal authorities of both organizations.[81] Posse Comitatus clearly limits military action within the confines of law enforcement, but has been adjusted to allow DoD support to interdicting illegal drugs coming into the U.S. Title 10 provides an example to extend specific DoD capabilities to defend cyber that would be consistent with current law such as allowing DoD equipment to support a response to a Weapons of Mass Destruction (WMD). It appears these specific situations were based on the robust DoD capability to offset local, state, and federal shortfalls which may also be the circumstance with DoD possessing the capacity that DHS lacks in the cyber domain. Specifying unique circumstances for DoD action such as WMD or cyber puts the weight of the DoD capacity to support the

homeland defense. Congress must pass any changes to U.S. Code enabling authorities, and the language could be added to allow DoD certain latitude to actively protect cyber in support of infrastructure like nuclear power plants.

Legal liabilities for private and public organizations that would share sensitive information on cyber disruptions and attacks with the federal government are not currently codified in law. This issue is at the center of sharing and passing key information on ongoing cyber events across all key sectors of the U.S. Most importantly, all decisions on the way forward must be made in the context of a complex environment and within the freedom, rights, and protection of all Americans.

Strategies

Central Control

One potential option to resolve the issue of cyber leadership for the nation is to employ a central position perhaps a cabinet level position, along with a newly created department who could oversee all government initiatives for cyber. Under the current construct, the White House Cyber Coordinator has no independent authority, no congressional budget, and only minimal staff to coordinate policy and strategy. In the current state of decreasing resources across the Federal Government, it would be doubtful to build another cabinet level position with a supporting staff to create a Secretary of Cyber for instance. Some have articulated a DoD approach as the executive agent, but the overarching challenges in limited authorities along law enforcement make this option doubtful. DHS maintains a likely department to provide oversight and executive agency if congressional legislation specified such authorities. Even in this potential solution, critical networks serving the defense of the nation controlled by DCI and DoD would be excluded from DHS authority, so there would still

be at least two distinct organizations protecting the government's networks. A structural challenge to a hierarchical response to a network challenge is that the bureaucracy could not keep up with the potential threats.

Open Strategy

As there are more stakeholders within cyber than can be named, perhaps a better position is to identify that everyone has a role in defending the national interests in cyber. For instance The Comprehensive National Cybersecurity Initiative includes an effort to link all of the appropriate cyber current operations centers to gain a common understanding of the environment.[82] Specific legal authorities must be clarified and spelled out in new legislation as there has been no substantive cyber legislation since 2002. In view of a central oversight and deconfliction authority, DHS could chair the whole of government action at this strategic level without impending on others. Legislation should allow sharing at the lowest levels between industry and government through computer to computer communications to stop threats to U.S. interests without concern of potential lawsuits. In this way, a public company could freely share details of ongoing disruptions with NSA without working through a middleman at DHS, as is the current structure because of limitations on DoD. Key participants such as DoD, DHS, and FBI would generally maintain the traditional lines of responsibility, but in a collaborative environment. Access to information, as well as action to stop an incident may come from law enforcement or defense organizations in an active defense scenario. As both nationally sponsored threats and private hackers intend to disrupt and attack U.S. interests, stopping the disruption as quickly as possible is the central issue. As mentioned previously, attribution can be challenging at best. Appropriate action could be taken to stop the hostile action without clearly identifying the what or

who originated the threat. In a more network-based response, the potential threat would be unaware of who was countering their attack; DoD, FBI, or private network administrators. Our adversaries know the very public limitations placed on DoD, so they can operate without worry of intervention by the military Broadening DoD's authorities in concert with DHS, and networking all the U.S. governments' capabilities has the potential to create unknowns for all adversaries as the U.S. government has even reserved kinetic responses to potential cyber threats. In those specific cases it would be a DoD response, but maintaining a level of ambiguity keeps all options on the table.

Recommendation

The breadth of the problem and complexity of the environment demands that not one organization bears the entire responsibility for protecting all U.S. interests in cyber, but rather a shared approach to detection and mitigation. In line with the bank robbery construct, where multiple organizations jointly work to stop the theft, maintaining a linked and coordinated cyber defense would allow the greatest flexibility in defending the interests of the U.S. Congressional action would codify the coordinating role for the whole of government approach lead by DHS as opposed to the ambiguity in the current laws. Modifications to the Telecommunications Act of 1984 would strike the legal classification of Internet activity as "law enforcement", replacing the language with a "threat to national interests". Specific language would be added to Posse Comitatus in line with the drug enforcement model to include cyber incidents, opening the potential for DoD to defend beyond their own networks. This addresses the fact that the military and government as a whole do not own the vast majority of the network they currently use today. Protection of U.S. companies and private organizations would enable real-time sharing and collaboration beyond the limits currently identified in the key and

critical infrastructure legislation. Prioritization of the threat with potential damage to U.S. interests and power would allow an immediate response. A legislated private/public organization could be put in place to provide oversight to minimize concerns about privacy that would go farther than the Presidential Executive Order of February 2013. The order directs the Chief Privacy Officer and the Officer for Civil Rights and Civil liberties of DHS to assess and provide mitigation for all DHS actions.[83] This could be an increase in the oversight of the Information Security and Privacy Advisory Board (ISPAB) as an already standing structure. The ISPAB "advises NIST, Secretary of Commerce, and the Director OMB on information and privacy issues."[84] Allowing increased DoD authority to act would necessitate DoD to increase membership on the ISPAB or similarly modeled private/public legislated committee beyond the NSA representative. Furthermore the committee would have greater latitude on potential oversight concerning privacy issues as example. Self-protection of private organizations would remain as the first line of defense just as in the bank scenario, but other network defenders would be observing real-time to provide back-up just like the FBI does today in every bank robbery.

Endnotes

[1] Department of Homeland Security, *Bottom-Up Review Report* (Washington, DC: US Department of Homeland Security, July 2010), 23.

[2] Homeland Security Studies and Analysis Institute, An Analysis of the Primary Authorities Supporting and Governing the Efforts of the Department of Homeland Security to Secure the Cyberspace of the United States, May 24, 2011, 1 http://www.homelandsecurity.org/docs/reports/MHF-and-EG-Analysis-of-authorities-supporting-efforts-of-DHS-to-secure-cyberspace-2011.pdf (accessed November 7, 2012).

[3] *Cornell University Law School Legal Information Institute*, 400 USC § 11103, http://www.law.cornell.edu/uscode/text/40/11103 (accessed January 19, 2013).

[4] Whitehouse National Security Council, "Cyberspace Policy Review," http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (accessed December 18, 2012).

[5] U.S. Strategic Command Home Page, http://www.stratcom.mil/factsheets/Cyber_Command (accessed November 7, 2012).

[6] *Senate Armed Services Committee Hearing*. Lanham, United States, Lanham: Federal Information & News Dispatch, Inc, 2012, http://search.proquest.com/docview/951609573?accountid=4444.ew/951609573?accountid=4444.

[7] Department of Homeland Security, "Napolitano's Remarks at the ASIS International 58th Annual Seminar," September 10, 2012, http://www.dhs.gov/news/2012/09/10/secretary-napolitano's-remarks-asis-international-58th-annual-seminar (accessed November 7, 2012).

[8] *House Energy and Commerce Subcommittee on Communications and Technology Hearing*. Lanham, United States, Lanham: Federal Information & News Dispatch, Inc, 2012, http://search.proquest.com/docview/920838191?accountid=4444.

[9] Mudrinich, Erik M. "Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem." *The Air Force Law Review* 68 (2012): 167-206, http://search.proquest.com/docview/1020878866?accountid=4444.

[10] Isaac R Porche, I.,II, M. Sollinger Jerry, and Shawn McKay. "An Enemy without Boundaries." *United States Naval Institute.Proceedings* 138, no. 10 (2012): 34-9, http://search.proquest.com/docview/1115098190?accountid=4444.

[11] Gary D. Brown and Owen W. Tullos, "On the Spectrum of Cyberspace Operations", *Small Wars Journal,* December 11, 2012, http://smallwarsjournal.com/jrnl/art/on-the-spectrum-of-cyberspace-operations (accessed January 10, 2013).

[12] Ibid.

[13] Ibid.

[14] Ibid.

[15] George W. Bush, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (Washington, DC: The White House, February 2003), 6.

[16] John Leyden, "UK.gov:Foreign Cyber Reconnaissance underway in UK, Eyes on Tentacles Peer from Network Pipes Around You," December 4, 2012, http://www.theregister.co.uk/2012/12/04/cyber_security_strategy/print.html (accessed December 5, 2012).

[17] James G. Stavridis and Elton C. Parker III, "Sailing the Cyber Sea," *Joint Forces Quarterly*, issue 65, 2nd Quarter (2012): 62.

[18] Bob Brewin, "Americans Want Defense—Not DHS—to Guard Cyberspace, Lawmakers Say," March 21,2012,http://www.nextgov.com/defense/2012/03/americans-want-defense-not-dhs-to-guard-cyberspace-lawmakers-say/50869/ (accessed November 12, 2012).

[19] US Chamber of Commerce, "Key Vote letter on S. 3414, the Cybersecurity Act of 2012", http://www.uschamber.com/issues/letters/2012/key-vote-letter-s-3414-cybersecurity-act-2012%E2%80%9D (accessed January 10, 2013).

[20] US Chamber of Commerce, "Critical Infrastructure Protection, Information Sharing and Cyber Security", http://www.uschamber.com/issues/defense/critical-infrastructure-protection-information-sharing-and-cyber-security (accessed January 10, 2013).

[21] Robert L. Mitchell, "The New Rules of Cyberwar," *Computerworld*, November 5, 2012, http://search.proquest.com/docview/1151858224 (accessed December 18, 2012).

[22] Ibid.

[23] Ibid.

[24] North American Aerospace Defense Command Home Page, http://www.norad.mil/about/index.html (accessed December 1, 2012).

[25] Strategic Command Fact Sheets, Home Page, http://www.stratcom.mil/factsheets/Cyber_Command (accessed December 1, 2012).

[26] Federal Bureau of Investigation (FBI) Investigate Reports of Major Thefts and Bank Robbery, http://www.fbi.gov/about-us/investigate/vc_majorthefts/bankrobbery (accessed December 2, 2012).

[27] Jared Serbu, "On Cyber Defense, U.S. 'Stuck at the Starting Line'," November 8, 2012, http://www.federalnewsradio.com/index.php?nid=851&sid=3110944 (accessed December 5, 2012).

[28] Homeland Security Studies and Analysis Institute, An Analysis of the Primary Authorities 3-4.

[29] George W. Bush, *Executive Order 13231: Critical Infrastructure Protection in the Information Age*, October 16, 2001, http://www.gpo.gov/fdsys/pkg/FR-2001-10-18/pdf/01-26509.pdf (accessed December 16, 2012), 1.

[30] Ibid.

[31] Homeland Security Studies and Analysis Institute, An Analysis of the Primary Authorities, 13.

[32] Department of Homeland Security Website, *National Infrastructure Advisory Council Members*, http://www.dhs.gov/national-infrastructure-advisory-council-members (accessed March 04, 2013).

[33] *Homeland Security Act of 2002,* Public Law 107-296, 107th Cong., (November 25, 2002), http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf (accessed December 5, 2012), 10.

[34] *Homeland Security Act of 2002, 12.*

[35] *Homeland Security Act of 2002, 13.*

[36] *Homeland Security Act of 2002, 16.*

[37] *Federal Information Security Management Act of 2002,* Public Law 107-347, 107th Cong., (December 17, 2002), http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf (accessed December 16, 2012).

[38] *Cornell University Law School Legal Information Institute*, US Code, http://www.law.cornell.edu/uscode/text/44/3542 (accessed December 16, 2012).

[39] Homeland Security Studies and Analysis Institute, An Analysis of the Primary Authorities, 12.

[40] George W. Bush, *Executive Order 13286: Amendment of Executive Orders, and Other Actions, in Connection With the Transfer of Certain Functions to the Secretary of Homeland Security*, February 28, 2003, http://www.gpo.gov/fdsys/pkg/FR-2003-03-05/pdf/03-5343.pdf (accessed December 9, 2012), 28.

[41] National Communications System Homepage, "National Security Telecommunications Advisory Committee (NSTAC), http://www.ncs.gov/nstac/ (accessed February 7, 2013).

[42] Ronald Reagan, *Executive Order 12472: Assignment of National Security and Emergency Preparedness Telecommunications Functions,* April 3, 1984, http://www.ncs.gov/library/policy_docs/eo_12472.html (accessed December 10, 2012).

[43] Ibid.

[44] George W. Bush, *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection,* December 17, 2003, http://www.dhs.gov/homeland-security-presidential-directive-7 (accessed December 5, 2012).

[45] Ibid.

[46] *Homeland Security Presidential Directive 7*

[47] Ibid.

[48] Whitehouse National Security Council, "Cyberspace Policy Review," http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (accessed December 18, 2012).

[49] Department of Homeland Security White Paper, "Computer Network Security & Privacy Protection," February 19, 2012,

http://www.dhs.gov/xlibrary/assets/privacy/privacy_cybersecurity_white_paper.pdf (accessed December 5, 2012), 2.

[50] Homeland Security Studies and Analysis Institute, *An Analysis of the Primary Authorities Supporting and Governing the Efforts of the Department of Homeland Security to Secure the Cyberspace of the United States* (Arlington, VA: Homeland Security Studies and Analysis Institute, May 24, 2011), 10.

[51] Paul Rosenzweig, "10 Conservative Principles for Cybersecurity Policy," *Backgrounder no.2513* January 31, 2011, http://www.heritage.org/research/reports/2011/01/10-conservative-principles-for-cybersecurity-policy#_ftnref28 (accessed January 21, 2013).

[52] Barack H. Obama, *Executive Order—Improving Critical Infrastructure Cybersecurity,* February 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (accessed March 4, 2013).

[53] Ibid.

[54] Ibid.

[55] United States Secret Service Webpage, *Criminal Investigations,* http://www.secretservice.gov/criminal.shtml (accessed January 21, 2013).

[56] John Moteff, *Computer Security: A Summary of Selected Federal Laws, Executive Orders, and Presidential Directive* (Washington, DC: U.S. Library of Congress, Congressional Research Service, April 16, 2004), 9.

[57] National Institute of Science and Technology (NIST) "General Information" from the NIST main website http://www.nist.gov/public_affairs/general_information.cfm (accessed January 19, 2013).

[58] "Cybersecurity Research and Development Act", January 23, 2002, http://csrc.nist.gov/drivers/documents/HR3394-final.pdf (accessed January 19, 2013).

[59] *Homeland Security Presidential Directive 7*

[60] Barack H. Obama, *Executive Order—Improving Critical Infrastructure Cybersecurity,* February 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (accessed March 4, 2013).

[61] White House Author Profile, *Michael Daniel, Special Assistant to the President and Cybersecurity Coordinator* http://www.whitehouse.gov/blog/author/Michael%20Daniel (accessed January 21, 2013).

[62] Associated Press, "White House Struggles to Fill Cyber Czar Post" , August 4, 2009, http://www.msnbc.msn.com/id/32290186/ns/politics-white_house/t/white-house-struggles-fill-cyber-czar-post/#.UP2b56XntUQ (accessed January 21, 2013).

[63] General Keith B. Alexander, U.S. Army, *State of Commander, U.S. Cyber Command before the Senate Committee on Armed Services,* March 27, 2012, 13, http://www.armed-services.senate.gov/statemnt/2012/03%20March/Alexander%2003-27-12.pdf (accessed December 16, 2012).

[64] Ibid

[65] Andru E. Wall, "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities and Covert Action," *Harvard National Security Journal*, Volume 3, January 2012, http://harvardnsj.org/wp-content/uploads/2012/01/Vol.-3_Wall1.pdf (accessed November 12, 2012).

[66] *Cornell University Law School Legal Information Institute*, 50 USC § 403–5, http://www.law.cornell.edu/uscode/text/50/403-5 (accessed December 18, 2012).

[67] *Cornell University Law School Legal Information Institute*, 10 USC §371, http://www.law.cornell.edu/uscode/text/10/371 (accessed December 16, 2012).

[68] Ibid.

[69] *Cornell University Law School Legal Information Institute*, 10 USC §113, http://www.law.cornell.edu/uscode/text/10/113?quicktabs_8=1#quicktabs-8 (accessed December 16, 2012).

[70] Demystifying the Title 10-Title 50 Debate,101.

[71] *Cornell University Law School Legal Information Institute*, 18 USC §1385, http://www.law.cornell.edu/uscode/text/18/1385?quicktabs_8=1#quicktabs-8 (accessed December 16, 2012).

[72] Charles Doyle, *The Posse Comitatus Act & Related Matters: The Use of the Military to Execute Civilian Law* (Washington, DC: U.S. Library of Congress, Congressional Research Service, April 16, 2004), 20-22, http://assets.opencrs.com/rpts/95-964_20000601.pdf (accessed December 19, 2012).

[73] Ronald W. Reagan, *Executive Order 12333: United States Intelligence Activities,* December 4, 1981, http://www.archives.gov/federal-register/codification/executive-order/12333.html (accessed December 16, 2012).

[74] Ibid

[75] Committee on National Security Systems (CNSS), *National Directive on Security of National Security Systems: CNSS Directive No. 502,* December 16, 2004, 2 http://www.cnss.gov/Assets/pdf/CNSSD-502.pdf (accessed December 21, 2012).

[76] The Committee on National Security Systems website, http://www.cnss.gov/history.html (accessed January 19, 2013).

[77] Ibid.

[78] *Executive Order 13231,* 2.

[79] Kevin P. Newmeyer, "Who Should Lead US Cybersecurity Efforts," *Prism 3, no 2*, February 12, 2012, http://www.ndu.edu/press/lib/pdf/prism3-2/prism115-126_newmeyer.pdf (accessed November 12, 2012) 115-126.

[80] Barack H. Obama, *Presidential Policy Directive 21, Critical Infrastructure Security and Resilience*, February 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (accessed March 4, 2013).

[81] Memorandum of Agreement between the Department of Homeland Security and Department of Defense Regarding Cyber Security, September 27, 2010, http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf (accessed February 7, 2013).

[82] Whitehouse National Security Council, "The Comprehensive National Cybersecurity Initiative," http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative (accessed February 7, 2013).

[83] Barack H. Obama, *Executive Order—Improving Critical Infrastructure Cybersecurity,* February 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (accessed March 4, 2013).

[84] US Department of Commerce National Institute of Standards and Technology, “Charter of the Information Security and Privacy Advisory Board” , http://csrc.nist.gov/groups/SMA/ispab/documents/ispab_charter-2012-2014.pdf (accessed February 7, 2013).